STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-028
September 2020

SURPLUS COMPUTER HARD DRIVE DISPOSAL PROCESSES

At Selected State Agencies

Sherrill F. Norman, CPA
Auditor General

State Agency Heads

The Florida Statutes establish the various State agencies and provide the title and selection process for the head of each State agency. The table below shows the four State agencies included in the scope of this information technology operational audit and the respective agency heads who served during the period of our audit.

State Agency	Established by Florida Statutes	State Agency Head
Agency for Health Care Administration	Section 20.42	Mary C. Mayhew, Secretary
Department of Business and Professional Regulation	Section 20.165	Halsey Beshears, Secretary
Department of Children and Families	Section 20.19	Chad Poppell, Secretary
Department of Education	Section 20.15 and Article IX, Section 2 of the State Constitution	Richard Corcoran, Executive Director and Commissioner of Education

The audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

SURPLUS COMPUTER HARD DRIVE DISPOSAL PROCESSES

At Selected State Agencies

SUMMARY

This operational audit focused on evaluating selected information technology (IT) controls applicable to the storage, sanitization, and disposal of surplus computer hard drives at the Agency for Health Care Administration (AHCA), the Department of Business and Professional Regulation (DBPR), the Department of Children and Families (DCF), and the Department of Education (DOE). This audit also included a follow-up on the findings in our report No. 2015-052 applicable to the DBPR. Our audit disclosed the following:

Finding 1: Certain security controls related to physical access at the DBPR, the DCF, and the DOE need improvement to ensure the continued protection of agency information.

Finding 2: AHCA and DCF physical access policies and procedures need enhancement to ensure that periodic reviews of physical access privileges to secure IT areas are conducted and the results of such reviews are maintained in agency records.

Finding 3: AHCA, DCF, and DOE procedures for tracking and maintaining records related to the sanitization and disposition of surplus computer hard drives need improvement.

BACKGROUND

To promote the appropriate disposal of surplus computers, it is important for State agencies to follow an orderly and controlled disposal process. Most importantly, when surplus computers are to be destroyed, repurposed, or made available by State agencies to other entities (e.g., donation to nonprofit organizations), appropriate procedures need to be followed to sanitize the surplus computer hard drives to ensure that confidential or exempt information is physically removed from the computer hard drives so that such information cannot be inadvertently or inappropriately disclosed. Department of Management Services (DMS) rules[1] require State agencies to formally manage assets throughout removal, transfer, and disposition by:

- Ensuring records on storage media to be disposed of or released for reuse are sanitized or destroyed in accordance with agency-developed procedures.
- Sanitizing or destroying confidential or exempt information such that the information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.
- Documenting procedures for sanitization of IT equipment prior to reassignment or disposal.

Acceptable sanitization methods for computer hard drives include erasure by overwriting (wiping) the data, degaussing (demagnetizing), or physical destruction.

[1] DMS Rule 60GG-2.003(4)(c)1. - 4., Florida Administrative Code.

Deleting files on surplus computer hard drives through normal system means does not physically remove data; it only removes the operating system's ability to locate the information. Unless appropriate sanitization methods are followed to overwrite, degauss, or physically destroy the computer drives, any information therein can be easily recovered using specialized commercially available software. This creates the risk that confidential or exempt information, should it reside on the computer hard drives, may be inappropriately disclosed.

Many Federal and State laws exist that limit the disclosure of certain information. For example, State law[2] provides that social security numbers held by an agency are confidential and exempt from public disclosure. Consequently, State agencies may not be in compliance with applicable State laws if due diligence is not exercised throughout the surplus computer hard drive disposal process.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Controls – Physical Access

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to physical access at the Department of Business and Professional Regulation (DBPR), the Department of Children and Families (DCF), and the Department of Education (DOE) need improvement to ensure that agency information is protected. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising those agencies' information. However, we have notified appropriate management of the specific issues.

Without adequate security controls related to physical access, the risk is increased that DBPR, DCF, and DOE information may be compromised. We communicated a similar finding to DBPR management in connection with our report No. 2015-052 (finding No. 1).

Recommendation: We recommend that DBPR, DCF, and DOE management improve security controls related to physical access to ensure the continued protection of agency information.

Finding 2: Periodic Review of Physical Access Privileges

DMS rules[3] require State agencies to manage and protect physical access to assets and, in doing so, establish security procedures to manage physical access to IT facilities and equipment. Management should also conduct regular (periodic) reviews of individuals with physical access to sensitive areas to ensure access is appropriate.

As part of our audit, we reviewed agency policies and procedures, examined agency records, and interviewed staff responsible for ensuring access to secured IT areas, including where surplus computers and hard drives awaiting sanitization and disposition were stored, was appropriate. As subsequently

[2] Section 119.071(5)(a)5., Florida Statutes.

[3] DMS Rule 60GG-2.003(1)(b)2., Florida Administrative Code.

described, our audit procedures disclosed that Agency for Health Care Administration (AHCA) and DCF physical access privilege review policies, procedures, and processes need improvement.

AHCA

To maximize the safety and security of individuals and facilities, AHCA policies and procedures[4] required management at the Bureau Chief level or above to review the security access needs of employees, consultants, and vendors. However, the policies and procedures did not establish the frequency for such access reviews and, according to AHCA management, as of January 27, 2020, a review of physical access privileges to the secured IT area where sensitive IT equipment, such as hard drives awaiting sanitization and disposition and servers, were stored had not been performed since February 2018. While access to the locked cabinet where the surplus hard drives were secured within the IT area was appropriately restricted, a periodic review of the secured IT area would ensure that access to all sensitive IT equipment remained appropriate.

DCF

To prevent the loss of confidentiality, integrity, or availability of information stored on computer equipment or media, DCF policies and procedures[5] specified that information system removable media was to be protected until the media was destroyed or sanitized using approved equipment, techniques, and procedures. However, the policies and procedures did not require periodic reviews of physical access privileges to the secured IT areas where surplus computers and hard drives awaiting sanitization and disposition were stored to help ensure access remained appropriate. According to DCF management, periodic physical access privilege reviews had not been conducted for two secured IT areas, Phillips Road and DCF Headquarters, evaluated as part of our audit that stored surplus computers and hard drives awaiting sanitization and disposition. Specifically, DCF management confirmed on January 17, 2020, that periodic physical access privilege reviews had never been conducted for the Phillips Road location. Further, DCF management indicated in response to our audit inquiry that, before initiating an ad hoc physical access privilege review of the DCF Headquarters location in January 2020, the last ad hoc review was conducted more than 3 years prior.

Effective policies and procedures for periodically reviewing physical access privileges to secured IT areas help protect surplus computers and hard drives awaiting sanitization and disposition and other sensitive IT equipment from inappropriate access and reduce the risk that confidential information may be compromised. Additionally, periodic reviews of physical access privileges increase management's assurance that the access privileges granted are authorized and remain appropriate.

Recommendation: We recommend that AHCA and DCF management improve physical access policies and procedures to require periodic physical access privilege reviews of secure IT areas and ensure that documentation of such reviews is maintained in agency records.

[4] AHCA Policy and Procedure No. 4029, *Security and Identification Badges*.

[5] DCF Operating Procedure CFOP 50-28, *Media Protection*.

Finding 3: Surplus Computer Hard Drive Sanitization and Disposition Procedures and Documentation

Effective security controls include the establishment of policies and procedures that describe management's expectations for controlling an organization's operations. Documented policies and procedures help ensure that management directives are clearly communicated, understood, accepted, and followed by all staff. DMS rules[6] require State agencies to formally manage assets throughout removal, transfer, and disposition by documenting procedures for sanitization of IT equipment prior to reassignment or disposal and ensuring that records on storage media to be disposed of or released for reuse are sanitized or destroyed in accordance with agency-developed procedures. Effective management of the sanitization and disposition of surplus IT equipment includes maintaining records of when IT equipment are added to the IT environment, when the IT equipment leave the place they were last used, when they reach the sanitization destination, when and how they were sanitized, and the final disposition.

Our review of the surplus computer hard drive sanitization and disposition procedures and documentation at AHCA, the DCF, and the DOE disclosed that surplus computer hard drive sanitization and disposition procedures and documentation need improvement.

AHCA

AHCA policies and procedures[7] required the Property Custodian to complete a *Request for Certification of Surplus Property* form (form) for computers that were obsolete, no longer in working condition, or were no longer needed. The policies and procedures also required the Division of Information Technology to sign the form acknowledging that all AHCA data had been removed from the computers; however, the policies and procedures did not require removed hard drive serial numbers, the number of hard drives removed, or any other identifying information to be documented. In practice, the Property Custodian contacted the Division of Information Technology to remove the hard drives from the surplus computers identified on the form prior to surrendering the computers to General Services for disposal or surplus. Division of Information Technology staff then delivered the removed hard drives to the IT Security Team to be stored for sanitization or destruction at a later date.

Our review of AHCA sanitization and disposition policies and procedures and the form found that AHCA policies and procedures and the form did not promote the association of removed hard drives to be sanitized to the originating computer or the serial numbers of removed hard drives to their final disposition (repurposed, destroyed, or donated). Specifically, we inspected two example completed forms and interviewed applicable staff and found that, at the time of removal, Division of Information Technology staff signed the forms certifying that all AHCA data had been deleted (sanitized) from the computers identified on the forms. However, when the forms were signed, the hard drives had not been sanitized and the serial numbers of the removed hard drives were not identified on the forms. Consequently, AHCA records did not evidence that all hard drives were accounted for and subsequently sanitized or destroyed. According to AHCA management, the form needed updating to accurately and completely reflect the

[6] DMS Rule 60GG-2.003(4)(c)1. - 4., Florida Administrative Code.

[7] AHCA Policy and Procedure No. 4007, *Property Management*.

surplus sanitization and disposition process, including a field to evidence quantity and serial number information for surplused hard drives.

DCF

DCF policies and procedures[8] required employees to ensure that data sanitization of any IT resource was performed prior to the disposal, surplus, reuse, or off-site repair of the resource and in accordance with applicable Federal and DCF standards and policies. The policies and procedures also required the sanitization process to remove information from the media such that the information could not be retrieved or reconstructed and required the information owner and the information custodian to review, approve, track, document, and verify media sanitization methods for computers containing Federal tax information. While these policies and procedures provided direction for the sanitization, disposition, and verification process, they did not require sufficiently detailed records be maintained to document and track the sanitization and disposition process. For example, information to identify the computers received for surplus, the date the computers were received, when and how the hard drives were sanitized, and the final disposition of the hard drives and computers was not maintained.

We interviewed DCF staff and inspected the available sanitization documentation and disposition records for the period January 2019 through October 2019 at DCF Headquarters and the DCF Daytona Beach Regional Facility and found that:

- At DCF Headquarters, DCF IT staff removed the hard drives upon receipt of the surplus computers and physically destroyed the hard drives. According to DCF IT management, records identifying the receipt of surplus computers, such as property or serial numbers or other identifying information, was not maintained. Additionally, DCF IT staff did not maintain records evidencing the destruction of hard drives, such as the number of hard drives removed, the serial numbers or other identifying information for the hard drives, the date hard drives were destroyed, and responsible staff.
- At the DCF Daytona Beach Regional Facility, when the IT section received used IT equipment, the equipment storage list was updated to reflect the receipt of the used IT equipment and the IT equipment was placed in storage. When a determination was made to surplus the used IT equipment, the IT equipment was reclassified as surplus, removed from the equipment storage list, and added to the surplus equipment list. For surplus computers, the hard drives were removed and were either physically destroyed, sanitized and put back in the surplus computers or, if the computers were being donated to DCF partners, the hard drives were removed, sanitized, reimaged, and put back in the surplus computers. While a spreadsheet was maintained by IT staff documenting the property and serial numbers of the originating computer, sanitization method for the hard drives, initials of the individual who performed the sanitization, and the date sanitization was performed, the spreadsheet did not track the number of hard drives removed and sanitized, serial numbers of the removed drives, or any other identifying information that associated the removed hard drives with the originating computer. Additionally, when IT equipment on the storage list was reclassified as surplus, the information was deleted from the storage list, inhibiting the ability to reconcile the equipment received and placed into storage to the equipment reclassified as surplus and precluding a complete accounting of IT equipment.

[8] DCF Operating Procedure CFOP 50-28, *Media Protection*.

DOE

Pursuant to DOE policies and procedures,[9] the General Services Property Section was responsible for overseeing the authorization for and disposal of all surplus property. The policies and procedures required applicable IT staff to be notified prior to designating computers as surplus and once designated as surplus, all computer hard drives were to be removed and sanitized (wiped or destroyed) by an IT technician. The policies and procedures specified that any hard drives determined to be usable were to be removed from the computer and become the property of the Division of Technology and Innovation for possible reuse, and the originating computers were to be labeled certifying that the hard drives were either removed or sanitized prior to disposal. Additionally, the Division of Technology and Innovation and DOE Division, Bureau, and Section Property Custodian Delegates had various informal procedures for disposing of surplus computers in accordance with DOE policies and procedures.

Our evaluation of formal and informal DOE policies and procedures found that, while the policies and procedures provided guidance for the sanitization and disposition of surplus computers, including requiring the completion of a certification form,[10] they did not require sufficiently detailed records be maintained to document and track the sanitization and disposition process. Our review of two example certification forms found that, while the form included fields to document a description of surplus computers, applicable serial and property numbers, and a signature indicating that hard drives had been sanitized, the certification form did not include fields to document the serial numbers or other identifying information of hard drives removed for sanitization to permit the hard drives to be associated with the originating computers. Also, the certification form did not include fields for the number of hard drives removed, sanitization method (i.e., wiped or destroyed), or the final disposition of the wiped hard drives (i.e., reinstalled in surplus computers for donation or retained for reuse by the DOE).

Effective policies and procedures for managing the surplus computer hard drive sanitization and disposition process help promote accountability and reduce the risk that AHCA, DCF, and DOE information may be compromised. Without complete records associating removed hard drives with the originating surplus computers and reconciliations to ensure that all removed hard drives are accounted for as sanitized or destroyed, management has reduced assurance over the information necessary to ensure proper accountability for and control over computer hard drives to prevent inappropriate or unauthorized access to confidential or exempt information.

Recommendation: We recommend that AHCA, DCF, and DOE management establish comprehensive policies and procedures for the surplus computer hard drive sanitization and disposition process and ensure that agency records appropriately account for and evidence the sanitization and disposition of all surplus computer hard drives.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the DBPR had taken corrective actions for the findings included in our report No. 2015-052.

[9] DOE Policy No. 8.9, *Property Management*.

[10] DOE Form GS7001, *Certification of DOE Surplus Property*.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from September 2019 through March 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant IT controls applicable to the storage, sanitization, and disposal of surplus computer hard drives at the Agency for Health Care Administration (AHCA), the Department of Business and Professional Regulation (DBPR), the Department of Children and Families (DCF), and the Department of Education (DOE) during the period October 2019 through March 2020 and selected actions prior and subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources as related to surplus computer hard drive disposal processes.
- To determine whether management had corrected, or was in the process of correcting, deficiencies applicable to the DBPR disclosed in our report No. 2015-052.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[11] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

[11] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Governor and AHCA, DBPR, and DCF Management and the Governor, State Board of Education, and DOE Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that the internal control components significant to our audit objectives included control environment, control activities, information and communication, and monitoring. The associated underlying principles significant to our objectives included:

- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve AHCA's, DBPR's, DCF's, and DOE's goals and objectives.
- Management design of control activities to achieve AHCA's, DBPR's, DCF's, and DOE's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management communication of information internally necessary to achieve AHCA's, DBPR's, DCF's, and DOE's objectives.
- Management activities to monitor AHCA's, DBPR's, DCF's, and DOE's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems

so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, AHCA, DBPR, DCF, and DOE policies and procedures, and other guidelines to obtain an understanding of IT controls applicable to the storage, sanitization, and disposal of surplus computer hard drives.
- Interviewed AHCA, DBPR, DCF, and DOE personnel.
- Obtained an understanding of AHCA, DBPR, DCF, and DOE procedures for approving, storing, and documenting surplus IT equipment for disposal.
- Obtained an understanding of AHCA, DBPR, DCF, and DOE specialized hardware, software, and specific processes used to ensure electronic storage media in surplus IT equipment are appropriately sanitized before disposal.
- Evaluated the adequacy of AHCA, DBPR, DCF, and DOE surplus IT equipment procedures and related records evidencing the approval of equipment identified as surplus and all relevant information, including the removal of confidential or exempt information from electronic media before the media is made available for reuse or disposal.
- Evaluated the effectiveness of physical access controls for the storage of computers and removed hard drives awaiting sanitization or destruction. Specifically, we:
    - Observed on various dates during the period November 14, 2019, through January 8, 2020, the physical access security controls for AHCA, the DBPR, the DCF, and the DOE.
    - Examined records and evaluated the adequacy of AHCA, DBPR, DCF, and DOE policies, procedures, and processes for reviewing physical security over surplus IT equipment storage areas.
    - Evaluated the appropriateness of access to the AHCA locked cabinets within the secured IT area as of November 14, 2019, for the 2 individuals granted access.

- Evaluated the appropriateness of access to the DBPR Tallahassee Office secured IT area as of November 22, 2019, for the 24 DBPR staff with assigned key cards and the 6 key cards assigned to the building management company.
- Evaluated the appropriateness of access to the DCF Headquarters secured IT area as of January 14, 2020, for the 58 individuals granted access.
- Evaluated the appropriateness of access to the DCF Daytona Beach Regional Facility secured IT area as of December 10, 2019, for the 5 DCF employees assigned a key and the shared key assigned to the DMS-contracted cleaning service.
- Evaluated the appropriateness of access to the DCF Tallahassee Regional Field Office secured IT area as of January 7, 2020, for the 2 individuals granted access.
- Evaluated the appropriateness of access to the DOE Turlington Building secured IT area as of January 24, 2020, for the 32 individuals granted access.
- Evaluated the appropriateness of access to the DOE Division of Blind Services Daytona Beach District Office secured IT area as of December 6, 2019, for the 6 individuals granted access.
- Evaluated the appropriateness of access to the DOE Division of Vocational Rehabilitation Orlando Field Office secured IT area as of December 16, 2019, for the 3 individuals granted access.

- Evaluated the adequacy of AHCA, DBPR, DCF, and DOE sanitization documentation and disposition records and the effectiveness of security controls over the sanitization process for electronic storage media in surplus computers. Specifically, to determine whether electronic storage media were properly erased, and all files were no longer readable, we evaluated the adequacy of the sanitization process for computer hard drives:
  - As of December 6, 2019, for 27 of the 140 computer hard drives available for disposal at AHCA.
  - As of December 3, 2019, for the 19 computer hard drives available for disposal at the DBPR.
  - As of December 3, 2019, for 12 of the 72 computers available for disposal at the DCF Daytona Beach Regional Facility.
  - As of November 26, 2019, for 15 of the 781 computers available for disposal at the DOE Turlington Building.
  - As of December 4, 2019, for 10 of the 65 computers and 10 of the 153 separately stored computer hard drives available for disposal at the DOE Division of Blind Services Daytona Beach District Office.
  - As of November 13, 2019, for 16 of the 67 computers available for disposal at the DOE Division of Vocational Rehabilitation Orlando Field Office.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's responses are included in this report under the heading ***MANAGEMENT RESPONSES***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

RON DESANTIS
GOVERNOR

MARY C. MAYHEW
SECRETARY

September 4, 2020

Ms. Sherrill F. Norman
Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Thank you for the opportunity to respond to the preliminary and tentative findings and recommendations from your information technology operational audit of Surplus Computer Hard Drive Disposal Processes at Selected State Agencies, including the Agency for Health Care Administration. In accordance with your request, we have emailed you the preliminary and tentative audit findings document with our response incorporated therein.

If you have any questions regarding our response, please contact Pilar Zaki, Audit Director, at 412-3986.

Sincerely,

Mary C. Mayhew
Secretary

MCM/sgb
Enclosure

2727 Mahan Drive • Mail Stop #1
Tallahassee, FL 32308
AHCA.MyFlorida.com

Facebook.com/AHCAFlorida
Youtube.com/AHCAFlorida
Twitter.com/AHCA_FL
SlideShare.net/AHCAFlorida

Finding 2:
Periodic Review of Physical Access Privileges. AHCA and DCF physical access policies and procedures need enhancement to ensure that periodic reviews of physical access privileges to secure IT areas are conducted and the results of such reviews are maintained in agency records.

Recommendation:
We recommend that AHCA and DCF management improve physical access policies and procedures to require periodic physical access privilege reviews of secure IT areas and ensure that documentation of such reviews is maintained in agency records.

Agency Response:
The AHCA Division of Operations, Bureau of Support Services has re-written Administrative Policy & Procedure (AP&P) #4029 Security and ID Badges (physical access policy).

Agency Contact
Scott Ward
(850) 412-4844

Brian Kenyon
(850) 412-3899

Finding 3:
Surplus Computer Hard Drive Sanitization and Disposition Procedures and Documentation. AHCA, DCF, and DOE procedures for tracking and maintaining records related to the sanitization and disposition of surplus computer hard drives need improvement.

Recommendation:
We recommend that AHCA, DCF, and DOE management establish comprehensive policies and procedures for the surplus computer hard drive sanitization and disposition process and ensure that agency records appropriately account for and evidence the sanitization and disposition of all surplus computer hard drives.

Agency Response:
The AHCA Division of IT has re-written policy AP&P #5007 Media Sanitation Policy as a result of working with the Florida Auditor General during this audit. The AHCA Division of Operations, Bureau of Support Services has also updated AP&P #4007 Property Management.

To ensure that agency records appropriately account for and evidence the sanitization and disposition of all surplus computer hard drives, the Bureau of Support Services is updating the "Request for Certification of Surplus Property Form" which includes the IT certification area to clarify wiping drives versus the removal of hard drives.

Agency Contact
Scott Ward
(850) 412-4844

Florida dbpr Department of Business & Professional Regulation

Division of Technology
Joseph Martin, Director
2601 Blair Stone Road
Tallahassee, Florida 32399-0781
Phone: 850.487.3094 • Fax: 850.921.4984

Halsey Beshears, Secretary

Ron DeSantis, Governor

September 9, 2020

Sherrill F. Norman, CPA
Auditor General
Claude Denson Pepper Building, G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, I have enclosed our response to the preliminary and tentative audit findings and recommendations related to the Information Technology (IT) Operational Audit of the Department of Business and Professional Regulation Surplus Computer Hard Drive Disposal Processes.

I wish to note that the similar finding from the 2015 audit pertained to a different DBPR location, and our records reflect it was successfully closed out.

We appreciate the work of your staff through the audit process, and thank you for your efforts to improve the security of state government.

If you have any questions concerning this response, please contact Lynne T. Winston, Inspector General, at (850) 414-6700.

Sincerely,

Joseph Martin
Chief Information Officer

cc: Thomas Philpot, Chief of Staff
Lynne T. Winston, Inspector General

Enclosure

Finding 1: Security Controls - Physical Access

Recommendation:
We recommend that DBPR management improve security controls related to physical access to ensure the continued protection of agency information.

Response:
We acknowledge the recommendation from the auditors and are reviewing our sanitization procedure to limit access to sensitive surplus equipment.

State of Florida
Department of Children and Families

Ron DeSantis
Governor

Chad Poppell
Secretary

September 21, 2020

Sherrill F. Norman, Auditor General
State of Florida Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Sherrill Norman:

Thank you for the opportunity to respond to your August 10, 2020 list of preliminary and tentative audit findings and recommendations from your information technology operational audit of *Surplus Computer Hard Drive Disposal Processes at Selected State Agencies, including the Department of Children and Families*. Enclosed is the response from our department.

Should you have any questions, please feel free to contact Chief Information Officer Julie Madden at (850) 320-9170.

Sincerely,

Chad Poppell
Secretary

Enclosure

cc: Keith R. Parks, Inspector General
David R. Mica, Chief of Staff
Julie Madden, Chief Information Officer
Tony Lloyd, Assistant Secretary for Administration
Matt Howard, General Services Director
Bonny Allen, Information Security Manager
Steven Meredith, Director of Auditing

/SM/ba

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS AUDITOR GENERAL OPERATIONAL AUDIT OF SURPLUS COMPUTER HARD DRIVE DISPOSAL PROCESSES AT SELECTED STATE AGENCIES

Finding No. 1: Certain security controls related to physical access at the DBPR, the DCF, and the DOE need improvement to ensure the continued protection of agency information.

Recommendation: The Florida Auditor General (AG) recommended that DBPR, DCF, and DOE management improve security controls related to physical access to ensure the continued protection of agency information.

Response: The Department's Information Security Manager (ISM) and appropriate staff selected from the Office of Information Technology Services (OITS) by the Department's Chief Information Officer (CIO) will meet with appropriate staff identified by the Department's Director of the Office of General Services to discuss this finding and identify the physical security controls that the Department needs to strengthen and further document in the Department's security and physical access policy and procedures which fall within the scope of authority of the CIO and by the Director. This review will include a review of the appropriate security controls from section 282.318, Florida Statutes (F.S.), *Security of Data and Information Technology*, Chapter 60GG-2, Florida Administrative Code (F.A.C.), *Information Technology Standards,* and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Estimated Completion Date: December 30, 2020

Finding No. 2: AHCA and DCF physical access policies and procedures need enhancement to ensure that periodic reviews of physical access privileges to secure IT areas are conducted and the results of such reviews are maintained in agency records.

Recommendation: The AG recommended that AHCA and DCF management improve physical access policies and procedures to require periodic physical access privilege reviews of secure IT areas and ensure that documentation of such reviews is maintained in agency records.

Response: The Department's ISM and appropriate staff selected by the Department's CIO will meet with the staff identified by the Department's Director of the Office of General Services to discuss this finding and identify the physical security controls that the Department needs to strengthen and further document in the Department's security and physical access policy and procedures which also fall within the scope of authority of the CIO and the Director. This review will also include the appropriate controls from section 282.318, F.S., *Security of Data and Information Technology*, Chapter 60GG-2, F.A.C., *Information Technology Standards*, NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Estimated Completion Date: December 30, 2020

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS AUDITOR GENERAL OPERATIONAL AUDIT OF SURPLUS COMPUTER HARD DRIVE DISPOSAL PROCESSES AT SELECTED STATE AGENCIES

Finding No. 3: AHCA, DCF, and DOE procedures for tracking and maintaining records related to the sanitization and disposition of surplus computer hard drives need improvement.

Recommendation: The AG recommended that AHCA, DCF, and DOE management establish comprehensive policies and procedures for the surplus computer hard drive sanitization and disposition process and ensure that agency records appropriately account for and evidence the sanitization and disposition of all surplus computer hard drives.

Response: The Department's ISM and staff selected by the Department's CIO will meet with the staff identified by the Department's Director of the Office of General Services to discuss this finding and document the actual sanitization process which should include the creation and retention of records about the sanitization and disposition of Department hard drives.

This review will include the appropriate controls from section 282.318, F.S., *Security of Data and Information Technology*, Chapter 60GG-2, F.A.C., *Information Technology Standards*, NIST SP 800-88 r1, *Guidelines for Media Sanitization*, and NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

These information security frameworks will be used to evaluate the Department's Office of General Services' policy, *ASG CFOP 80-2 Property Management*, and the CIO's standard operating procedure, *OITS SOP C-2: Reuse of Computer Storage Drives*, to identify opportunities for improvement that ensure sufficient records are maintained about hard drive sanitization and disposition.

Estimated Completion Date: December 30, 2020

September 9, 2020

Sherrill F. Norman, CPA
Florida Auditor General
Claude Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

The following responses are offered with respect to the preliminary and tentative audit findings issued August 10, 2020, on the information technology operational audit of Surplus Computer Hard Drive Disposal Processes at Selected State Agencies, including the Florida Department of Education (DOE):

Finding 1: Security Controls – Physical Access
Recommendation: We recommend that DOE management improve security controls related to physical access to ensure the continued protection of agency information.

Response: DOE concurs with the finding. The department has corrected this issue by securing access to surplus computers and hard drives awaiting sanitization and disposition to only staff requiring access for these assigned job responsibilities, in a secured room.

Finding 3: Surplus Computer Hard Drive Sanitization and Disposition Procedures and Documentation
Recommendation: We recommend that DOE management establish comprehensive policies and procedures for the surplus computer hard drive sanitization and disposition process and ensure that agency records appropriately account for and evidence the sanitization and disposition of all surplus computer hard drives.

Response: DOE concurs with the recommendation and, as such, the Division of Technology and Innovation has revised the Standard Operating Procedures (Media Sanitization Procedures) to account for and evidence the sanitization and disposition of all surplus hard drives.

If you have any questions, please contact Mike Blackburn, Inspector General, at 850-245-0403.

Sincerely,

Richard Corcoran
Commissioner of Education

RC/sg

cc: Suzanne Pridgeon, Deputy Commissioner, Finance and Operations
Andre Smith, Deputy Commissioner of Innovation, Division of Technology and Innovation
Mike Blackburn, Inspector General
Robert Doyle, Director, Division of Blind Services
Mari M. "Miki" Presley, Assistant Deputy Commissioner, Finance and Operations
Sean Freeman, Educational Program Director